AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for ensuring that data generated by a client, ~~an untrusted entity,~~ comprising a first computing device, and subsequently stored in a persistent storage of the ~~untrusted entity~~client have not been modified when the data are subsequently accessed for use by the ~~untrusted entity~~client, the method comprising: ~~steps of:~~

(a) the ~~untrusted entity~~client sending first data related information to ~~the trusted entity~~ a server for signature computation;

(b) ~~a trusted entity,~~the server, comprising a second computing device, computing a signature for the first data related information by ~~employing~~ utilizing a secure signing algorithm and a key that is only known and available for use by the ~~trusted entity~~server;~~, to compute a signature for the first data related information before the data are stored in the persistent storage by the untrusted entity;~~

(c) the ~~trusted entity~~server sending the signature to the ~~untrusted entity~~client for storage;

(d) the client storing both the signature and the data in the persistent storage of the ~~untrusted entity~~client;

(e) before the data that were stored are subsequently used by the ~~untrusted entity~~client, the ~~untrusted entity~~client sending both second data related information and the signature to the ~~trusted entity~~server to verify that the data that were stored have not been changed;

(f) the ~~trusted entity~~server generating a temporary signature of the second data related information by utilizing the secure signing algorithm and the key that is only known and available for use by the ~~trusted entity~~server; ~~to generate a temporary signature of the second data related information sent to the trusted entity;~~

(g) the server comparing the temporary signature to the stored signature; ~~and~~

(h) when the temporary signature is equal to the stored signature, sending a positive result to the client;

(i) when the temporary signature is not equal to the stored signature, sending a negative result to the client;

(j) the client receiving the result from the server and evaluating the result;

(k) when the result is positive, the client using the data; and

(l) when the result is negative, the client not using the data.

~~(h) only using the data that were stored if the step of comparing indicates that the signatures match and that the data that were stored have not been changed since the signature was computed before storing the data and the signature.~~

2. (Currently Amended) The method of Claim 1, wherein the first data related information is the same as the data. ~~and the second data related information is the same as the stored data.~~

3-4. (Canceled)

5. (Currently Amended) The method of Claim 1, wherein the first data related information comprises a digest of the data calculated by the client using a one-way hash function and the data, and the second data related information comprises a digest of the stored data calculated by the client using a one-way hash function and the stored data. ~~wherein the digests are calculated by the untrusted entity based on the data and stored data.~~

6-7. (Canceled)

8. (Currently Amended) The method of Claim 5, wherein the first data related information further comprises:

(a) a signer identification (SID) for the ~~untrusted entity~~client, the ~~signer (ID)~~SID uniquely identifying the ~~untrusted entity~~client and not being controlled by an operator of the ~~untrusted entity~~client;

9-10. (Canceled)

11. (Currently Amended) The method of Claim 1, wherein the data comprise a plurality of different sets of data, further comprising the steps of:

(a) obtaining a signer identification (SID) for the ~~untrusted entity~~client, the ~~signer ID~~SID uniquely indicating the ~~untrusted entity~~client and not being controlled by an operator of the ~~untrusted entity~~client;

(b) on the ~~trusted entity~~server, using the key for computing an intermediate key from a concatenation of an arbitrary value and the ~~signer ID~~SID;

(c) sending the intermediate key from the ~~trusted entity~~server to the ~~untrusted entity~~client;

(d) using the intermediate key to sign each set of the data to produce the signature for the set of data; and

(e) storing the signature, the arbitrary value, and the ~~signer ID~~SID on the persistent storage.

12-13. (Canceled)

14. (Currently Amended) The method of Claim 11, further comprising the step of determining if the ~~signer ID~~SID that was received from the ~~untrusted entity~~client is on a list of banned ~~signer IDs~~SIDs, and if so, indicating in the result that the set of data are not usable by the ~~untrusted entity~~client.

15-18. (Canceled)

19. (Original) A memory medium on which machine readable instructions are stored for carrying out the steps of Claim 1.

20. (Currently Amended) A ~~untrusted entity~~client, comprising a first gaming device, in which game session related data for use by the gaming device in subsequent gaming sessions are stored, the client further comprising:

(a) a memory in which machine instructions are stored;

(b) a persistent storage used to store data;

(c) a network interface adapted to link the ~~untrusted entity~~client in communication over a network with a ~~trusted entity~~server, comprising a second computing device; ~~over a network;~~ and

(d) a processor coupled to the memory, the persistent storage, and the network interface, said processor executing the machine instructions to carry out a plurality of functions, including:

(i) ~~before storing~~sending game session related data, to the server ~~obtaining~~ to obtain a signature from the ~~trusted entity~~server for the data, the signature ~~determined~~ calculated by the server using the game session related data and a key known only by a ~~trusted entity~~server and not available to the ~~untrusted entity~~client;

(ii) receiving from the server the signature;

(iii) storing the game session related data and the signature received from the server in the persistent storage;

~~(iii)~~(iv) before using the game session related data that were stored in the persistent storage, obtaining a ~~verification~~ result from the ~~trusted entity~~server ~~that~~ indicating whether the game session related data have not been altered, the result being obtained by:

a) sending the game session related data and the signature to the server,

b) the server calculating a new signature of the game session related data and comparing the new signature with the signature,

c) when the new signature equals the signature, receiving a positive result from the server,

d) when the new signature does not equal the signature, receiving a negative result from the server; ~~as a function of the signature; and~~

(v) when the result is positive, using the game session related data; and

(vi) when the result is negative, not using the game session related data.

~~(iv) only using the game session related data that were stored if the step of obtaining the verification indicates that the game session related data that were stored have not been changed since the signature was computed by the trusted entity before storing the game session related data and the signature.~~

21. (Currently Amended) The ~~untrusted entity~~client of Claim 20, wherein the machine instructions further cause the processor to compute a digest of the game session related data before the game session related data are stored in the persistent storage, said digest being sent to ~~a trusted entity~~the server for computing the signature.

22. (Currently Amended) The ~~untrusted entity~~client of Claim 21, wherein the machine instructions further cause the processor to store a signer identification (SID) that is used in computing the signature, the ~~signer ID~~SID uniquely identifying the ~~untrusted entity~~client and being uncontrolled by the ~~untrusted entity~~client or an operator of the ~~untrusted entity~~client, so that the signature establishes a relationship between the game session related data before the game session related data are stored and the ~~signer ID~~SID.

23. (Currently Amended) The ~~untrusted entity~~client of Claim 20, wherein the game session related data comprises a plurality of sets of game session related data, and wherein the machine instructions further cause the processor to:

(a) request an intermediate key from ~~a trusted entity~~the server for use in computing a signature of each set of the game session related data before the set is stored in the persistent storage, the intermediate key being determined as a function of a signer identification (SID) and an arbitrary value, the ~~signer ID~~SID uniquely identifying the ~~untrusted entity~~client and being uncontrolled by the ~~untrusted entity~~client or an operator of the ~~untrusted entity~~client, said ~~untrusted entity~~client receiving the intermediate key, the arbitrary value, and the ~~signer ID~~SID;

(b) computing a digest of each set of the game session related data;

(c) computing the signature of the digest for each set of the game session related data using the intermediate key; and

(d) storing the signature, the arbitrary value, and the ~~signer ID~~SID in the persistent storage.

24. (Currently Amended) The ~~untrusted entity~~client of Claim 23, wherein before using the game session related data that were stored, the machine instructions further cause the processor to compute a temporary digest of the game session related data that were stored; and then send the temporary digest, and the signature, the arbitrary value, and the ~~signer ID~~SID that were stored to ~~a trusted entity~~the server for verification that the game session related data and the ~~signer ID~~SID have not been changed.

25 – 26. (Canceled)

27. (Currently Amended) A ~~trusted entity~~server, comprising a first computing device, that is employed in determining whether data stored in a persistent storage on a client which comprises ~~an untrusted entity, comprising~~ a second computing device, have been altered since the data were initially stored, the server further comprising:

(a) a memory in which machine instructions are stored;

(b) a network interface adapted to link the ~~trusted entity~~server in communication over a network with a ~~untrusted entity~~client; ~~over a network;~~ and

(c) a processor coupled to the memory, and the network interface, said processor executing the machine instructions to carryout a plurality of functions, including:

(i) receiving the data from the client;

(ii) computing a signature for the data by utilizing ~~employing~~ a key that is only known and available for use by the ~~trusted entity~~server ~~to compute a signature for the data~~ before the data are stored in a persistent storage by ~~a untrusted entity~~the client;~~,~~

(iii) sending ~~said~~ the signature ~~being sent~~ to the client ~~a untrusted entity and~~ to be stored in a persistent storage in association with the data; ~~and~~

(iv) receiving second data and the signature from the client;

(vi) computing a temporary signature using the second data and the key that is only known and available for use by the server;

(v) comparing the temporary signature and the signature;

(vii) when the temporary signature is equal to the signature, sending a positive result to the client; and

(viii) when the temporary signature is not equal to the signature, sending a negative result to the client.

~~(ii) before the data that were stored are subsequently used by a untrusted entity, utilizing the key known only to the trusted entity to compute a temporary signature for the stored data to facilitate a verification that the data that were stored have not been altered.~~

28. (Cancelled)

29. (Currently Amended) The ~~trusted entity~~server of Claim 27, wherein the machine instructions further cause the processor to compute the signature based upon a digest of the data that is to be stored, where the digest is received from the client. ~~an untrusted entity.~~

30. (Currently Amended) The ~~trusted entity~~server of Claim 27, wherein the machine instructions further cause the processor to use the key in determining the signature from a concatenation of a digest of the data that is to be stored and a signer identification (SID) uniquely identifying a ~~untrusted entity~~client on which the data are to be stored, wherein the ~~signer ID~~SID is uncontrolled and unalterable by the ~~untrusted entity~~client and an operator of the ~~untrusted entity~~client, the ~~signer ID~~SID being sent by the ~~trusted entity~~server to the ~~untrusted entity~~client with the signature.

31. (Currently Amended) The ~~trusted entity~~server of Claim 30, wherein the machine instructions further cause the processor to receive a temporary digest of the data that had been stored on a ~~untrusted entity~~client and the ~~signer ID~~SID that had been stored on the ~~untrusted entity~~client, and compute a temporary signature of a concatenation of the ~~signer ID~~SID and the temporary digest using the key, and then to verify whether the data or the ~~signer ID~~SID that were stored were altered, by comparing the temporary signature with the signature, before sending a result of the comparison to the ~~untrusted entity~~client.

32. (Currently Amended) The ~~trusted entity~~server of Claim 27, wherein the machine instructions further cause the processor to respond to a request for an intermediate key from a ~~untrusted entity~~client by computing the intermediate key from an arbitrary value and a signer identification (SID) uniquely identifying the ~~untrusted entity~~client, wherein the ~~signer ID~~SID is uncontrolled and unalterable by the ~~untrusted entity~~client and an operator of the ~~untrusted entity~~client, the trusted entity then sending the intermediate key, the arbitrary value, and the ~~signer ID~~SID to the ~~untrusted entity~~client to enable the ~~untrusted entity~~client to store the arbitrary value, and the ~~signer ill~~SID and to use the intermediate key to sign each of a plurality of sets of the data before storing the sets of the data.

33. (Currently Amended) The ~~trusted entity~~server of Claim 32, wherein the machine instructions further cause the processor to:

(a) receive a temporary digest of a set of data that had been stored, along with the signature, the arbitrary value, and the ~~signer ID~~SID that were stored;

(b) compute a temporary intermediate key by using the key to sign the ~~signer ID~~SID and the arbitrary value that were received;

(c) compute a temporary signature for the set of data using an intermediate key;

(d) compare the temporary signature and the signature to verify whether the set of data or the ~~signer ID~~SID that have been stored have been altered; and

(e) sending a result of the comparison to the ~~untrusted entity~~client.

34 – 36. (Canceled)